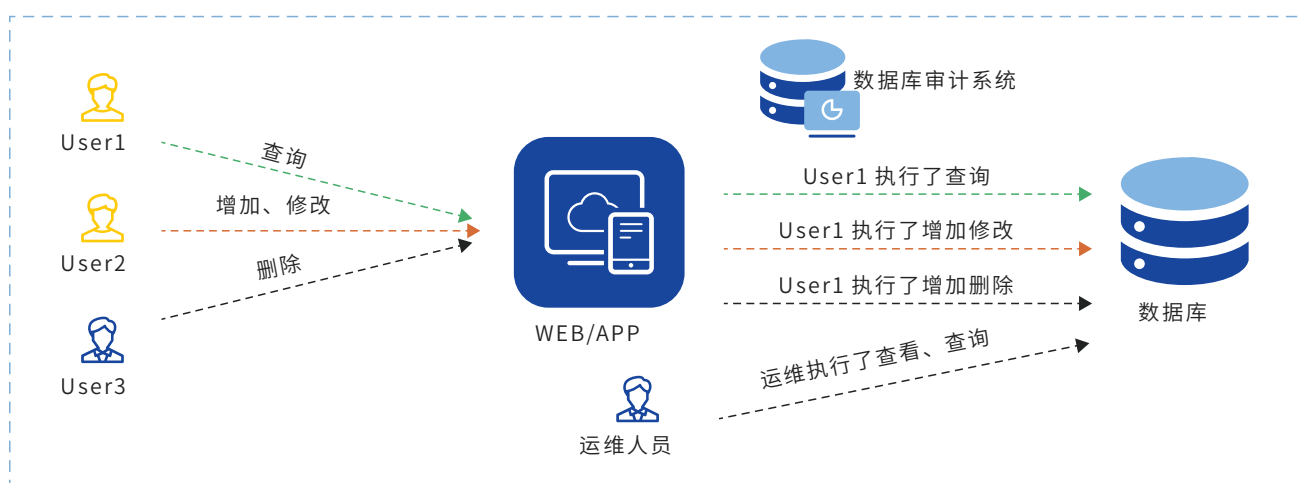


奇安信数据库审计与防护系统（数审）

奇安信网神数据库审计与防护系统支持软硬一体硬件，也支持软件形态部署在云 / 虚拟化 / 大数据等环境的一系列数据安全产品。审计系统采用数据库深度报文协议解析技术、DPI 和 DFI 动态流检测技术等，将数据库的各种操作，解析还原成原始的数据库语句，通过匹配预置的安全规则，智能分析和监控访问者的各种操作，进行实时威胁预警，并对事件统计分析记录，多重身份定位，有效支持电子取证。

主打功能



(1) 虚拟化及云环境部署：

- **针对问题：**客户的数据库服务器部署在云环境或者虚拟化环境中，无法采用端口镜像方式进行数据库报文信息采集。
- **解决方案：**提供≤5M 的报文引流装置，在数据库服务器部署 agent 插件将数据库操作行为报文引流到数据库审计系统中，进行数据库操作的分析和审计。

(2) 数据库访问监控与风险分析：

- **针对问题：**数据库管理人员常常无法实时感知企业内部具体的数据库账号分布，数据使用、内部员工在日常操作过程中是否存在运维误操作导致误删库、表；是否存在内外勾结进行的攻击，撞库、拖库等行为导致的数据泄露；以及是否存在外部直接进行 SQL 注入攻击这些风险操作行为；现有企业存在的态势感知、日志服务器、安全管理中心等平台都是针对网络进行的安全防护，没有只针对数据库操作访问进行审计的安全防护工具，形成的审计结果不全面。
- **解决方案：**通过内置数据库高危操作规则库、以及 SQL 注入的 CVE 漏洞库，识别并监控数据库访问风险，并通过邮件、短信等方式告警。同时数据库审计支持通过日志检索溯源数据安全事件，支持通过报表、行为轨迹图等方式可视化展示数据使用、数据访问风险的情况；支持通过 syslog 等接口可以向其他平台推送审计信息。



(3) 数据库自动扫描发现：

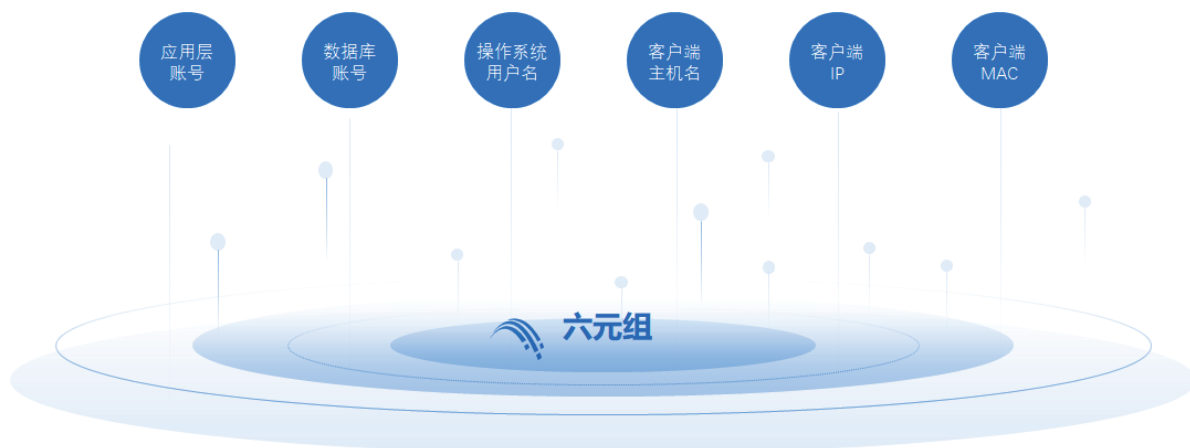
- **针对问题：**随着客户的业务发展，使用的应用系统越来越多，第三方维护人员是否有私自搭建数据库系统去使用，下级单位新上的应用有无上报到上级单位。造成管理人员无法清楚知道数据库的分布及使用情况，无法准确统计。
- **解决方案：**根据设定 IP 与端口范围以及网络报文协议解析，可以自动扫描出对应的数据库资产信息，一键添加保护对象，操作简单快捷，协助用户进行数据库资产梳理。

(4) 等保报表快速生成：

- **针对问题：**等保中有关于数据库审计报表的要求，客户每次导出数据的时候需要设置查询条件才能完成导出，都是一些固定且重复性的操作，费时又费力。
- **解决方案：**在进行等保报表导出时无需重复执行查询动作，可根据等保中关于审计报表的相关要求，将查询条件组合化生成查询模板，一键导出符合等保要求的报表。

(5) 关联审计精准定位到具体的操作人员：

- **针对问题：**用户操作数据时，中间经过应用系统，数据库自身的审计无法得知具体的操作人员信息。
- **解决方案：**审计系统支持 B/S、C/S，以及带 COM/DCOM/COM+ 组件方式的三层关联审计。支持独创组件关联技术，将 url 信息与操作语句信息关联提取工号（账号），精准定位到具体的客户端操



（6）敏感数据的操作行为规范

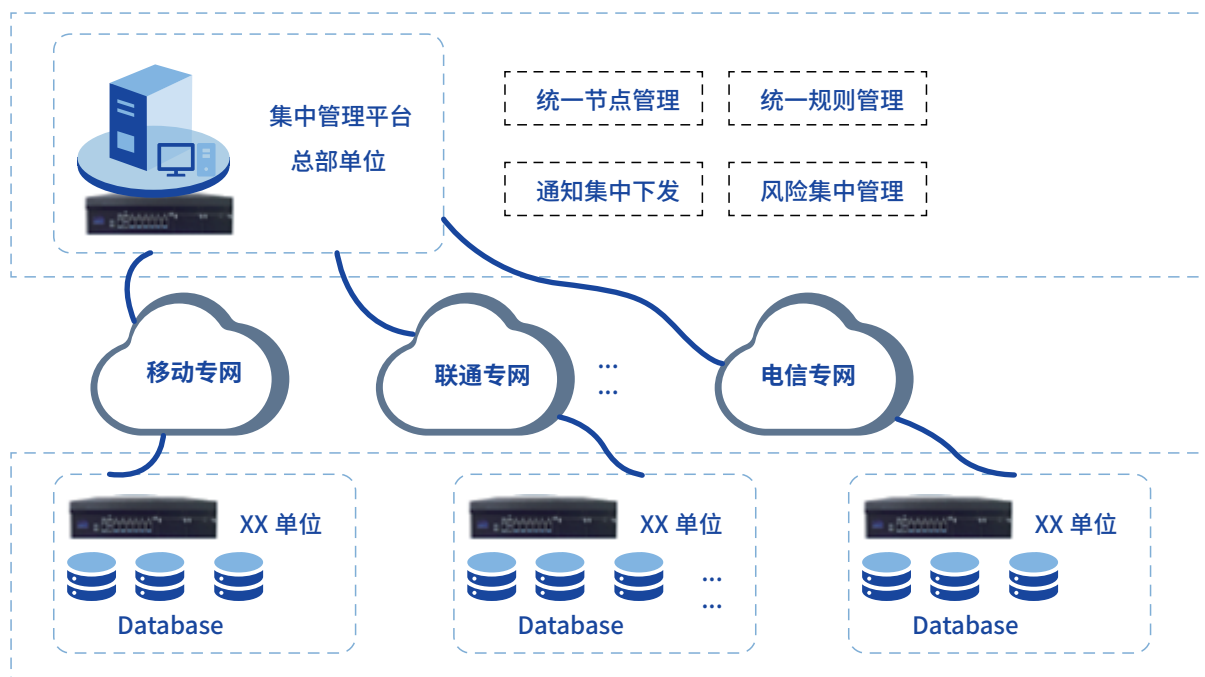
- 针对问题：**在进行数据库操作审计时，执行的是双向审计，可以查看到具体的访问返回结果信息，返回结果中有可能包含了客户的敏感信息，在展示审计记录时可造成数据的二次泄露。
- 解决方案：**数据库审计系统在进行数据库安全审计前，自动扫描出敏感数据分布信息，用户根据扫描出的敏感数据信息设置访问规则，客户端访问数据库时触发了敏感数据访问规则，在记录返回结果数据时，对涉及到的敏感数据进行脱敏处理，防止敏感数据的泄露。

（7）特殊环境下的数据库审计

- 针对问题：**企业在运行过程中，因业务需求使用的非常见数据库类型，如大数据，工控时序数据库，传统的审计无法满足审计的需求。
- 解决方案：**系统可通过解析 hadoop 平台的组件协议（hbase\impala\kafka\hive 等）实现大数据的审计。通过对工控数据库的报文解析，可审计工控数据库通过 WEB 和 API 调用等方式进行的操作。

（8）分布式部署集中管理

- 针对问题：**下属分支机构多，数据库审计设备多，信息科无法集中管理，审计信息混乱，审计规则无法统一制定。
- 解决方案：**数据库审计与防护系统支持分级部署，全局查询。对多层级部署的数据库实现全面、精确审计，统一管理，高效分析、快速检索。



应用场景

(1) 协助通过等保合规

- 场景问题：**在客户过等保时，等保要求对数据库的操作行为审计记录，记录日志信息保存 6 个月，同时需提供电子追溯文档。
- 解决方案：**部署数据库审计与防护系统，对数据库的访问进行全记录，同时可开启风险告警策略，进行实时告警外发和定时生成报表，审计记录可按等保要求时效保存完整地电子溯源文件。

(2) 协助抓出医院统方行为黑手

- 场景问题：**医院内外部人员勾结，违规出售或泄露医疗信息，纪委需要对此类行为精准定位到具体的操作人员。
- 解决方案：**数据库审计与防护系统可在不影响医疗应用系统正常使用的前提下，通过对客户端，应用端，数据库的操作行为进行关联分析，能够准确描述何人、何时、何地、以何种方式进行违规统方，并提供操作过程回放，供相关人员分析。

(3) 防范工控行业违规操作数据库行为

- 场景问题：**工控 MES 系统中的数据存储在一个工控时序数据库中，MES 系统若出现了违规操作，将直接影响到整个生产链条，造成不可挽回的损失。
- 解决方案：**数据库审计与防护系统通过分析工控数据库独有的通讯协议，还原成真实的 SQL 操作语句并进行详细的记录。一旦有 SQL 注入、高危操作等触发审计规则的事件，审计系统会及时发出告警信息通知管理员，避免数据库遭到进一步的破坏，并将整个过程的操作行为进行记录，以方便事后追踪溯源。

(4) 数据中心海量数据操作行为审计

- 场景问题：**在大型企业中，数据中心可能存在大量数据库（几百或几千），企业不想每个数据库进行单独审计，想集中审计所有的数据库，统一分析，统一管理。
- 解决方案：**针对超过海量的数据库操作行为需要审计，又想将审计信息统一管理，可以采取集群审计的方式。集群化部署后自动将流量分流到各审计节点，在不同的节点中报文信息处理完成后，统一在 WEB 平台进行展示，海量日志检索速度可达亿级数据秒级出检索结果。

(5) 分级部署集中管理

- 场景问题：**大型组织或机构一般拥有多个分支机构，各个分支机构的数据库服务器部署在不同的网络中，部署审计系统后，也是各自为阵，是否有使用，有合理地使用，上级单位无法对各个数据库审计系统的使用情况进行管理。
- 解决方案：**数据库审计与防护系统支持分级部署，全局查询，同时数据库审计集中管理平台支持进行统一的设备管理、策略下发、审计数据分析。